

EL887746245

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

**Multiple Trust Modes for Handling Data**

Inventors:

Jeremy Sokolic

Sanjeev Dheer

Venkatachari Dilip

ATTORNEY'S DOCKET NO. CE1-007US

1 **TECHNICAL FIELD**

2 The present invention relates to the handling data and, more particularly, to  
3 the use of multiple trust modes that define the manner in which certain data is  
4 handled.

5  
6 **BACKGROUND**

7 Users that interact with online services that involve, for example, financial  
8 data or financial transactions (e.g., accessing financial accounts, or buying or  
9 selling goods or services) are often required to provide data to the online service.  
10 This data may include bank account numbers, credit card numbers, passwords, and  
11 the like. Many existing online services store the data provided by the users of the  
12 online services. Some users may not be comfortable with their data being stored  
13 by a third party and, as a result, are reluctant to use the online services offered by  
14 these third parties. Thus, users are often faced with the decision to allow their  
15 data to be stored by a third party or to forego the services offered by the third  
16 party.

17 Similar problems occur with other types of online accounts and online  
18 relationships where credentials are issued to a user. With these types of accounts,  
19 when the user's credentials are stored, for example, on a server associated with the  
20 online account or other online service, those credentials are at risk of being  
21 accessed by an unauthorized person, thereby compromising the security of the  
22 user's account.

23 The systems and methods described herein address these and other  
24 problems by providing multiple trust modes that allow a user to determine how the  
25 user's data is handled.

1  
2 **SUMMARY**

3       The system and methods described herein provide users of online services  
4 with multiple options regarding how the user's data is handled. A particular  
5 option is selected by each user based on that user's level of trust in the system or  
6 organization that is handling the user's data. Certain options allow the system or  
7 organization to store the data while other options require the system or  
8 organization to avoid persistently storing the data when finished processing the  
9 user's request or transaction.

10       A particular embodiment presents a user with multiple modes of operation.  
11 The multiple modes of operation define different trust options for handling  
12 sensitive data associated with the user. A selection is received from the user,  
13 where the selection is one of the multiple modes of operation. The sensitive data  
14 associated with the user is handled in accordance with the selected mode of  
15 operation.

16       In one embodiment, the multiple modes include a low trust option that  
17 retrieves sensitive data from the user each time the user requests a service  
18 requiring the sensitive data.

19       In another embodiment, the multiple modes include a moderate trust option  
20 that retrieves sensitive data from the user and stores the sensitive data in an  
21 encrypted format using a password known only to the user.

22       In a particular embodiment, the multiple modes include a high trust option  
23 that retrieves sensitive data from the user and stores the sensitive data in an  
24 encrypted format for future use.  
25

## **BRIEF DESCRIPTION OF THE DRAWINGS**

Fig. 1 illustrates an exemplary network environment in which various servers, computing devices, and a financial analysis system exchange data across a network, such as the Internet.

Fig. 2 is a block diagram showing exemplary components and modules of a financial analysis system.

Fig. 3 is a flow diagram illustrating a procedure in which a user registers an account with the financial analysis system.

Fig. 4 is a flow diagram illustrating a procedure for automatically updating user accounts having a High Trust Mode of operation.

Fig. 5 is a flow diagram illustrating a procedure for updating one or more user accounts.

Fig. 6 is a flow diagram illustrating a procedure for allowing financial institutions to select among multiple trust modes that are made available to customers of the financial institutions.

Fig. 7 is a block diagram showing pertinent components of a computer in accordance with the invention.

## **DETAILED DESCRIPTION**

The systems and methods described herein provide various modes of operation that determine how user data is handled. A particular mode of operation is selected by each user based on the user's level of trust in the system or organization that is handling the data. A high level of trust allows the system or organization to store data, such as user credentials and other sensitive data, for

1 later use. A moderate level of trust allows the system or organization to store  
2 sensitive data in an encrypted format using a key derived from the user's password  
3 (i.e., the user associated with the sensitive data). A low level of trust does not  
4 allow the system or organization to store any sensitive data persistently. A user  
5 can change the level of trust associated with a particular account to reflect changes  
6 in their attitude toward the system or organization.

7 As used herein, the terms "account holder", "customer", "user", and  
8 "client" are interchangeable. "Account holder" refers to any person having access  
9 to an account. A particular account may have multiple account holders (e.g., a  
10 joint checking account having husband and wife as account holders or a corporate  
11 account identifying multiple corporate employees as account holders). Various  
12 financial account and financial institution examples are provided herein for  
13 purposes of explanation. However, it will be appreciated that the system and  
14 procedures described herein can be used with any type of asset account, any type  
15 of debt account, and any type of financial institution. Example asset accounts  
16 include savings accounts, money market accounts, checking accounts (both  
17 interest-bearing and non-interest-bearing), certificates of deposit (CDs), mutual  
18 funds, bonds, and equities. Example debt accounts include credit card accounts,  
19 mortgage accounts, home equity loans, overdraft protection, margin accounts,  
20 personal loans, and other types of loans. Exemplary financial institutions include  
21 banks, savings and loans, credit unions, mortgage companies, mutual fund  
22 companies, lending companies, and stock brokers.

23 Various financial account and financial institution examples are provided  
24 herein for purposes of explanation. However, the methods and procedures  
25 described herein can be applied to any type of transaction involving any type of

1 account. For example, a data aggregation system may aggregate data from  
2 multiple sources, such as multiple financial accounts, multiple email accounts,  
3 multiple online award (or reward) accounts, multiple news headlines, and the like.  
4 Similarly, the data retrieval and data processing systems and methods discussed  
5 herein may be applied to collect data from any type of account containing any type  
6 of data. Thus, the methods and systems described herein can be applied to a data  
7 aggregation system or any other account management system instead of the  
8 financial analysis system discussed in the examples provided herein.

9 Although particular examples discussed herein refer to the handling of a  
10 user's "sensitive data", the methods and systems described herein may be applied  
11 to any type of data associated with a user, an organization or other entity.

12 Fig. 1 illustrates an exemplary network environment 100 in which various  
13 servers, computing devices, and a financial analysis system exchange data across a  
14 data communication network. The network environment of Fig. 1 includes  
15 multiple financial institution servers 102, 104, and 106 coupled to a data  
16 communication network 108, such as the Internet. Each of the financial institution  
17 servers 102, 104, and 106 are typically associated with a particular financial  
18 institution and store data for that financial institution, such as customer account  
19 data. As shown in Fig. 1, a client computer 110 and a financial analysis system  
20 112 are also coupled to network 108. A database 114 is coupled to financial  
21 analysis system 112 for storing various data used by the financial analysis system.

22 Network 108 may be any type of data communication network using any  
23 communication protocol. Further, network 108 may include one or more sub-  
24 networks (not shown) which are interconnected with one another. Although only a  
25

1 few devices are shown coupled to network 108 in Fig. 1, a particular network may  
2 include any number of devices coupled to one another.

3 The communication links shown between the network 108 and the various  
4 devices (102-106 and 110-112) shown in Fig. 1 can use any type of  
5 communication medium and any communication protocol. For example, one or  
6 more of the communication links shown in Fig. 1 may be a wireless link (e.g., a  
7 radio frequency (RF) link or a microwave link) or a wired link accessed via a  
8 public telephone system or another communication network. Certain devices,  
9 such as servers, may be coupled to a local area network (LAN), which is coupled  
10 to network 108. Client computer 110 may access network 108 in different ways.  
11 First, client computer 110 may directly access network 108, for example, by using  
12 a modem to access a public telephone network (e.g., a public switched telephone  
13 network (PSTN)) that is coupled to network 108.

14 Financial analysis system 112 performs various analysis and data  
15 integration functions with respect to user accounts. These analysis functions are  
16 discussed in greater detail below. Client computer 110 allows a user to access  
17 information via the network 108. Client computer may be any type of computing  
18 device, such as a laptop computer, desktop computer, personal digital assistant  
19 (PDA), cellular phone, or set top box. For example, the user can access account  
20 information from one of the financial institution servers 102, 104, or 106, or send  
21 a request for an analysis or summary of the user's financial accounts to financial  
22 analysis system 112.

23 In a particular embodiment, the methods and systems described herein  
24 provide an Internet-based server solution where the sensitive data of one or more  
25 users is stored on a server, not a client.

1 Fig. 2 is a block diagram showing exemplary components and modules of  
2 financial analysis system 112. A communication interface 202 allows the  
3 financial analysis system 112 to communicate with other devices, such as one or  
4 more financial institution servers and client computers. In one embodiment,  
5 communication interface 202 is a network interface to a local area network (LAN),  
6 which is coupled to another data communication network, such as the Internet.

7 A database access module 204 allows financial analysis system 112 to store  
8 data to database 114 and retrieve data from the database. Financial analysis  
9 system 112 also stores various financial institution data 206, which may be used to  
10 locate and communicate with various financial institution servers. Financial  
11 institution data 206 includes, for example, Uniform Resource Locators (URLs)  
12 and login parameters.

13 A data extraction module 208 retrieves (or extracts) data from web pages or  
14 other data sources. The data extraction module 208 may use one or more data  
15 harvesting scripts 212 (also referred to as screen scraping scripts) to retrieve data  
16 from a web page or other data source. Data harvesting (or screen scraping) is a  
17 process that allows a script to retrieve data from one or more web pages associated  
18 with a web site. The retrieved data may be stored in a database, such as database  
19 114 (Fig. 1). The data harvesting scripts are capable of navigating web sites and  
20 capturing individual HTML pages. Typically, JavaScript and images are removed  
21 from the HTML pages or converted into HTML text if it contains account  
22 information. A parser then converts the HTML data into a field-delimited XML  
23 format. Data is then extracted from the XML format and stored in a database or  
24 other storage mechanism.  
25



1 Financial analysis system 112 also includes user account data 210 and a  
2 data handling module 214. User account data 210 typically includes information  
3 regarding the types of accounts are maintained by particular users as well as the  
4 locations of the accounts (i.e., the financial institution that handles the account)  
5 and account balances. The user account data 210 may also indicate the level of  
6 trust associated with each user account. User account data 210 may be stored in  
7 database 114 coupled to financial analysis system 112. Data handling module 214  
8 determines how account data is handled based on the level of trust associated with  
9 the account data and other factors.

10 Fig. 3 is a flow diagram illustrating a procedure 300 in which a user  
11 registers an account with the financial analysis system. Initially, a user generates a  
12 request to have the financial analysis system monitor one or more of the user's  
13 accounts (block 302). The financial analysis system then collects information  
14 from the user regarding the user accounts to be monitored (block 304). This  
15 information may include, for example, an account number, password to access the  
16 account online, the financial institution associated with the account, and the name  
17 or names listed on each account. The financial analysis system then presents the  
18 user with three different trust options for handling sensitive data associated with  
19 the user (block 306). This sensitive data may include, for example, the account  
20 number and password used to access the account online. In a particular  
21 embodiment, the sensitive data is the user login data (e.g., the username and  
22 password used to access an account). Although various examples discussed herein  
23 offer three different trust options for handling sensitive data, alternate  
24 embodiments may include fewer trust options or a greater number of trust options  
25

1 depending on the preferences of the users and/or the administrators of the financial  
2 analysis system.

3 In a particular embodiment, the three different trust options for handling  
4 sensitive data are referred to as “High Trust Option”, “Moderate Trust Option”,  
5 and “Low Trust Option”.

### 6 7 High Trust Option

8 A user selects the High Trust Option if the user is comfortable with having  
9 the financial analysis system store the user’s sensitive data. When this option is  
10 selected, the financial analysis system stores the user’s sensitive data for future  
11 use, such as automatically updating the user’s account balances. The user’s  
12 sensitive data is stored using a two-way data encryption technique, which allows a  
13 user key (derived from the user’s password) or a key maintained by the financial  
14 analysis system to decrypt the sensitive data. In one embodiment, the user’s  
15 sensitive data is encrypted using a Triple DES (Data Encryption Standard)  
16 algorithm. The Triple DES algorithm is a variation of the DES standard and has  
17 been endorsed by the National Institute of Standards and Technology (NIST).  
18 Triple DES uses three 64-bit keys, for an overall key length of 192 bits. The  
19 encryption procedure is similar to DES, but it is repeated three times. The data is  
20 encrypted with the first key, decrypted with the second key, and encrypted again  
21 with the third key.

22 Since the financial analysis system stores the user’s account number and  
23 password, the system is then able to automatically retrieve the user’s account  
24 balances using, for example, the data harvesting procedure discussed above.

1  
2  
3 Moderate Trust Option

4 A user selects the Moderate Trust Option if they are not comfortable with  
5 the High Trust Option, but don't want to have to enter their sensitive information  
6 each time they access the financial analysis system. When this option is selected,  
7 the financial analysis system stores the user's sensitive information, but the  
8 sensitive information is encrypted such that the information can only be decrypted  
9 when the user is online (i.e., logged into the financial analysis system). For  
10 example, the data can be encrypted using a key derived from the user's password.  
11 This encryption technique is referred to as one-way encryption because only one  
12 key (associated with the user's password) can decrypt the sensitive data. A  
13 particular embodiment of the one-way encryption uses HMAC-MD5. HMAC  
14 (Keyed-Hashing Message Authentication) is a mechanism for message  
15 authentication using cryptographic hash functions. HMAC can be used with any  
16 iterative cryptographic hash function, such as MD5. This combination is referred  
17 to as HMAC-MD5. MD5 is a message digest function, which is a function that  
18 takes a variable-length message and produces a fixed-length hash. MD5 is an  
19 example of a public one-way hash function.

20 When the user logs into the financial analysis system, the system  
21 automatically decrypts the user's sensitive information, which can then be used to  
22 retrieve updated information regarding the user's financial accounts.  
23

24 Low Trust Option  
25

1 A user selects the Low Trust Option if they are not comfortable with the  
2 financial analysis system storing any of the user's sensitive data. When this option  
3 is selected, the user's sensitive data is not persistently stored by the financial  
4 analysis system. Thus, the user must re-enter the sensitive data each time the user  
5 logs into the financial analysis system.

6 Referring again to Fig. 3, at block 308 the user selects one of the three trust  
7 options for each user account. The user may select a different trust option for  
8 different accounts or different financial institutions. For example, the user may  
9 assign a High Trust Option to a savings account and assign a Moderate Trust  
10 Option to a brokerage account. The financial analysis system then stores the  
11 selected trust option for each account (block 310). This information is stored, for  
12 example, in database 114. The trust option associated with each of the user's  
13 institutions can be retrieved from the database each time the user logs into the  
14 financial analysis system.

15 Fig. 4 is a flow diagram illustrating a procedure 400 for automatically  
16 updating user accounts having a High Trust Mode of operation. Initially, the  
17 procedure 400 determines whether it is time to perform automatic account updates  
18 (block 402). For example, High Trust Mode accounts may be updated  
19 automatically each business day. Other accounts may be updated hourly, weekly,  
20 monthly, or at other time intervals. In one embodiment, the account updates are  
21 performed as batch processes at predetermined times. If one or more automatic  
22 account updates are due to be performed, the financial analysis system identifies  
23 account information associated with High Trust Mode accounts (block 404). The  
24 system then retrieves current account information from all High Trust Mode  
25 accounts (block 406), e.g., using the data harvesting procedure discussed above.

1 The system then updates the various account information in the database with the  
2 retrieved information (block 408). The procedure then returns to block 402 to  
3 await the next automatic account update time. Thus, all user accounts that are  
4 designated High Trust Mode are automatically accessed to retrieve current account  
5 balances and other information. This retrieved data may be aggregated with data  
6 retrieved from other accounts using any data retrieval process.

7 Fig. 5 is a flow diagram illustrating a procedure 500 for updating one or  
8 more user accounts. Initially, a user logs on to the financial analysis system (block  
9 502). The user then requests to refresh account information (block 504). The  
10 financial analysis system identifies the user's account information, which includes  
11 decrypting the user's sensitive data (block 506). The procedure 500 then  
12 determines whether any of the user's accounts are Low Trust Mode accounts  
13 (block 508). If at least one of the user's accounts is a Low Trust Mode account,  
14 the financial analysis system asks the user for the missing credential (block 510),  
15 such as the user's password. As discussed above, the financial analysis system  
16 does not store any of the user's sensitive data related to Low Trust Mode accounts.  
17 Therefore, the user must provide the user ID and password, and explicitly request  
18 that the financial analysis system retrieve the current account information from the  
19 Low Trust Mode accounts. In alternate embodiments, the financial analysis  
20 system stores the user ID associated with Low Trust Mode accounts, but requires  
21 the user to enter the appropriate password each time the account is accessed.

22 The procedure then retrieves the current account information from all of the  
23 user's accounts, including Low Trust Mode accounts, Moderate Trust Mode  
24 accounts, and High Trust Mode accounts (block 512). The financial analysis  
25 system then updates the account information contained in the database with the

1 retrieved information (block 514). In one embodiment, only Moderate Trust Mode  
2 accounts are updated when the user logs on to the financial analysis system. In  
3 other embodiments, the financial analysis system may also update the user's High  
4 Trust Mode accounts and/or the user's Low Trust Mode accounts.

5 Fig. 6 is a flow diagram illustrating a procedure 600 for allowing partners  
6 to select among multiple trust modes that are made available to customers of the  
7 partners. A partner may be any organization that implements, for example, the  
8 systems described herein. Alternatively, a partner may be an organization that has  
9 the various services described herein implemented by another on behalf of the  
10 organization. Further, a partner may be an organization that provides a portal to  
11 another web site, such as a web site that implements the systems described herein.  
12 An organization that hosts a web site having an online registration requirement  
13 may also be a partner.

14 In certain situations, the financial analysis system provides data aggregation  
15 functions for one or more partners. These partners may want to limit the number  
16 of trust modes that are offered to their customers. Initially, the financial analysis  
17 system notifies one or more partners of the multiple trust modes available to users  
18 (block 602). Each partner then determines which trust modes should be made  
19 available to its customers (block 604). For example, a particular partner might not  
20 want to be responsible for storing the user's sensitive data in a two-way encrypted  
21 format (High Trust Mode) and doesn't want to offer that option to its customers.  
22 Each partner communicates the selected trust modes to the financial analysis  
23 system (block 606). The financial analysis system maintains a listing of all  
24 partners and their associated trust modes (block 608). This listing may be stored,  
25 for example, in database 114 (Fig. 1). Before allowing a user to set up a new

1 account with the financial analysis system, the system first checks to see if the  
2 partner associated with the new account (if any) has any restrictions on the types  
3 of trust modes available to its customers. If there are restrictions, the customer's  
4 choices are limited to those trust modes authorized by the partner.

5 Fig. 7 is a block diagram showing pertinent components of a computer 700  
6 in accordance with the invention. A computer such as that shown in Fig. 7 can be  
7 used, for example, to perform various procedures such as those discussed herein.  
8 Computer 700 can also be used to access a web site or other computing facility to  
9 access various financial information. The computer shown in Fig. 7 can function  
10 as a server, a client computer, or a financial analysis system, of the types discussed  
11 herein.

12 Computer 700 includes at least one processor 702 coupled to a bus 704 that  
13 couples together various system components. Bus 704 represents one or more of  
14 any of several types of bus structures, such as a memory bus or memory controller,  
15 a peripheral bus, and a processor or local bus using any of a variety of bus  
16 architectures. A random access memory (RAM) 706 and a read only memory  
17 (ROM) 708 are coupled to bus 704. Additionally, a network interface 710 and a  
18 removable storage device 712, such as a floppy disk or a CD-ROM, are coupled to  
19 bus 704. Network interface 710 provides an interface to a data communication  
20 network such as a local area network (LAN) or a wide area network (WAN) for  
21 exchanging data with other computers and devices. A disk storage 714, such as a  
22 hard disk, is coupled to bus 704 and provides for the non-volatile storage of data  
23 (e.g., computer-readable instructions, data structures, program modules and other  
24 data used by computer 700). Although computer 700 illustrates a removable  
25 storage 712 and a disk storage 714, it will be appreciated that other types of

1 computer-readable media which can store data that is accessible by a computer,  
2 such as magnetic cassettes, flash memory cards, digital video disks, and the like,  
3 may also be used in the exemplary computer.

4 Various peripheral interfaces 716 are coupled to bus 704 and provide an  
5 interface between the computer 700 and the individual peripheral devices.  
6 Exemplary peripheral devices include a display device 718, a keyboard 720, a  
7 mouse 722, a modem 724, and a printer 726. Modem 724 can be used to access  
8 other computer systems and devices directly or by connecting to a data  
9 communication network such as the Internet.

10 A variety of program modules can be stored on the disk storage 714,  
11 removable storage 712, RAM 706, or ROM 708, including an operating system,  
12 one or more application programs, and other program modules and program data.  
13 A user can enter commands and other information into computer 700 using the  
14 keyboard 720, mouse 722, or other input devices (not shown). Other input devices  
15 may include a microphone, joystick, game pad, scanner, satellite dish, or the like.

16 Computer 700 may operate in a network environment using logical  
17 connections to other remote computers. The remote computers may be personal  
18 computers, servers, routers, or peer devices. In a networked environment, some or  
19 all of the program modules executed by computer 700 may be retrieved from  
20 another computing device coupled to the network.

21 Typically, the computer 700 is programmed using instructions stored at  
22 different times in the various computer-readable media of the computer. Programs  
23 and operating systems are often distributed, for example, on floppy disks or CD-  
24 ROMs. The programs are installed from the distribution media into a storage  
25 device within the computer 700. When a program is executed, the program is at



1 least partially loaded into the computer's primary electronic memory. As  
2 described herein, the invention includes these and other types of computer-  
3 readable media when the media contains instructions or programs for  
4 implementing the steps described below in conjunction with a processor. The  
5 invention also includes the computer itself when programmed according to the  
6 procedures and techniques described herein.

7 For purposes of illustration, programs and other executable program  
8 components are illustrated herein as discrete blocks, although it is understood that  
9 such programs and components reside at various times in different storage  
10 components of the computer, and are executed by the computer's processor.  
11 Alternatively, the systems and procedures described herein can be implemented in  
12 hardware or a combination of hardware, software, and/or firmware. For example,  
13 one or more application specific integrated circuits (ASICs) can be programmed to  
14 carry out the systems and procedures described herein.

15 Although the description above uses language that is specific to structural  
16 features and/or methodological acts, it is to be understood that the invention  
17 defined in the appended claims is not limited to the specific features or acts  
18 described. Rather, the specific features and acts are disclosed as exemplary forms  
19 of implementing the invention.  
20  
21  
22  
23  
24  
25